SecureAge

NIST Protectフレームワークにおける暗号化の評価

SecureAgeホワイトペーパー2020

今日のITセキュリティとフレームワーク

今日では、さまざまなサイバーセキュリティフレームワークが存在し、異なるセクターのITセキュリティーを厳密かつ制御された方法で取り組む支援が行われています。例として、ISO IEC 27001 / ISO 27002、米国のNIST サイバーセキュリティ フレームワーク、英国のNISレギュレーション サイバー アセスメント フレームワークなどが挙げられます。これらは、企業がセキュリティの脅威からネットワークとコンピューターシステムを守るためのプロセス、実践、およびテクノロジーを含む定義されたフレームワークを通じて、効果的なサイバーセキュリティ戦略を実装、そして維持する優れた方法と言えるでしょう。

攻撃はそれでもすり抜ける: サイバーセキュリティのフレームワークにどれだけ時間と予算を費やしても、攻撃はそれをすり抜けて、データは盗まれます。すべてのデータ侵害を排除することは不可能ですが、暗号化技術は情報損失と組織への影響を最小限に食い止めることができます。その方法を、このホワイトペーパーで説明します。

> 「一部のマルウェアが通過する事実を受け入れることは、サイバー攻撃の被害にあってしまった時のための計画 立案、そして生じる損害を最小限に抑えるのに役立ちます。」
>
> 英国の国家サイバーセキュリティセンター

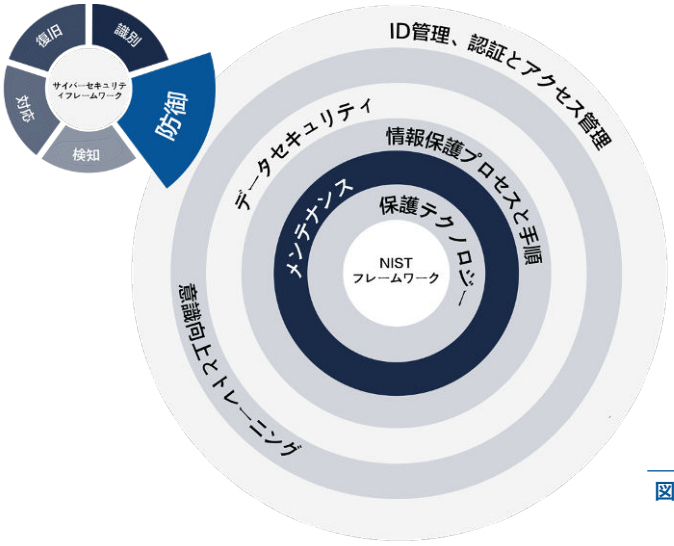

図1 NIST フレームワーク

本文書の構成

サイバー セキュリティ フレームワークの中心となる機能: サーバー攻撃からの保護: ここでは、NISTのフレームワークを用いて議論を展開しますが、提起された問題は、どのサイバーセキュリティフレームワークにも等しく当てはまります。

以下では、NISTのフレームワークの機能である「PROTECT（防御）」の6つのカテゴリーを挙げ、それぞれのカテゴリーで一般的に導入されている技術について検証します。各技術について、よく見られるデータ侵害のシナリオを説明し、次にデータ損失と盗難に焦点を当て、より広範囲なセキュリティ上の懸念について見ていきます。そして、SecureAgeの製品の一つであるSecureDataが、それぞれの問題に対して、どのような解決策を提供できるかを説明していきます。

SecureAgeのSecureDataは、最も基本的なファイルレベルの暗号化により、データを保護します。データへの不正アクセスをブロックしたり、保護するデータを選択したりする他のサイバー セキュリティ製品とは異なり、SecureDataは暗号化を利用して、本質的にファイル内のすべてのデータを守る製品であることを覚えておいてください。

NIST カテゴリー 1
ID管理、認証とアクセス制御

ID管理および認証システム

ユーザーログイン、シングルサインオン、多要素認証システムといったシステムは、権限を与えられた人のみが、システムやネットワークにアクセスできるように設計されています。リモートデスクトップ環境では、リモートマシンがすでにマルウェアに感染している可能性があり、アクセスを試みる者が物理的に自分の行動を隠すことなくアクセスできるため、特に脆弱性が高く、強力な認証が重要です。

データ漏えいのシナリオ

正当なユーザーがアプリケーションのデータをローカルファイルにコピーやダウンロードを行います。このファイルは、既にアプリケーションまたはデータベース内のコントロールによる保護の範囲にはありません。ファイルは簡単に盗まれる可能性があります。

> 英国のスーパーマーケット、Morrisonsの上級監査人は、恨みにより会社に損害を与えようとして、約10万人の従業員の給与データを漏洩しました。このデータは、簡単に抽出可能でした。データベースアプリケーションからエクスポートされ、ローカルファイルに保存されたのです。

セキュリティ上の懸念

データの盗難とユーザーアカウント侵害: ユーザーは、仕事をするために機密情報にアクセスする 必要があります。したがって、データを盗むのに理想的な立場にあります。不正な従業員も、侵害されたユーザーアカウントも同様です。

セキュリティ上の懸念の解決

情報はどこにコピーされたとしても、悪用から保護しなければなりません。そのためには、内部関係者によってファイルが盗まれた場合や、ユーザーアカウントが侵害された場合でも、データは安全に保たれている必要があります。ファイル内のデータが根本から保護されていれば、たとえ盗まれた情報であっても保護された状態が継続します。

SecureAgeのSecureDataを使用した場合、ユーザーは引き続き通常どおりに作業できますが、作業しているファイルはその裏側で暗号化されています。つまり、ファイルが盗まれてもデータ暗号化が継続するため、盗まれた情報を守ることができます。SecureDataはリモートデスクトップ環境でもデータの暗号化を実施し、SharePointやその他のWebDAVベースのサービスにおいても、情報はアプリケーションからサーバーやクラウドストレージまで、暗号化されて安全に保管されます。

アクセス制御リスト（ACL）

アクセス制御リスト（ACL）と最小特権の原則は、個人が仕事をするために必要な情報へのアクセスのみを提供することです。この原則は、データベースやアプリケーションにも適用されます。GDPRなどのデータ保護規制では、データを処理する正当な理由がある個人だけが、作業できるようにすべきであるとされています。管理者はそのような正当な必要性を持っていないため、アクセス制限の対象となる必要があります。

データ漏えいのシナリオ

特権を持つユーザーは知的財産を含むファイルにアクセスすることができますし、一般ユーザーでもファイルへの正当なアクセス権を持っている場合（仕事をするために必要なアクセス権）は、簡単にファイルを盗むことができます。NSAにおけるエドワード・スノーデンの行動は、おそらくこの種の最も注目を集める出来事です。

> データ侵害により、約36万人のケベック州の教師の個人情報が流出しました。ハッカーは、ユーザーコードとパスワードを盗み、データへのアクセスを可能にし、その盗難は簡単でした。

セキュリティ上の懸念

データへの特権ユーザーアクセス: ACLを利用する場合の多くで、特権を持つユーザーは、企業が閲覧を許可しないファイルへもアクセスできます。これは、管理者などがファイルの移動、バックアップの復元などを行うのに必要なためと思われます。ACLをセットアップした特権ユーザーは、自分が有利になるように変更もできるので、不正な管理者によって悪用される可能性も生まれます。そして、どのようなファイルでも、一度組織の管理から移動してしまえば、ACLの対象ではなくなり、保護はされません。

セキュリティ上の懸念の解決

SecureAgeのSecureDataを用いると、各ファイルがアクセス権限のある個人によって、暗号化されます。これはもちろん、アクセス制御とともに行われる必要があります。しかし、データが盗まれたとしても、SecureDataで保護された環境から持ち出されたファイルは暗号化されたままなので、組織の外では役に立ちません。たとえ盗んだ人物が、データにアクセスできる内部関係者であったとしても、復号できません。

NIST カテゴリー 2
意識向上とトレーニング

サイバーセキュリティ意識

サイバーセキュリティの意識向上トレーニングは、組織のITセキュリティア対策の重要な要素です。従業員、請負業者、関連するサードパーティーに、ネットワーク、システム、データを保護を遵守させるためは、シンプルですが強力なステップです。しかし、新入社員にプライバシーとデータ保護に関する意識向上トレーニングを実施している企業はわずか49%であり、定期的な再教育を実施している企業は4分の1未満にとどまっています。[1]

データ漏えいのシナリオ

攻撃者は、ソーシャルメディア、企業プレスリリースおよびブログなどを利用して、注意深く企業の経営層を監視しています。その情報をもとにして、ターゲットにメールが送信されます。このメールには、本物らしく見える特定の情報が含まれており、幹部は有害なリンクをクリックします。一見、何も起こらないように見えますが、裏側にはハッカーのバックドアを開くマルウェアが仕込まれており、データの窃盗を可能にします。

> Travelexは、ランサムウェア攻撃に遭い、数週間に渡り手作業での処理を余儀なくされました。法人顧客は通貨サービスを提供 することができなくなり、利用者は現金を引き出すことができませんでした。顧客情報も盗まれたと報告されており、ディスラプティブウェアの関与を示しています。

セキュリティ上の懸念

有害なアイテムを開封してしまう: 多忙やプレッシャーによって、人はミスをします。そして、スピアフィッシング攻撃やソーシャルネットワーキングサービスがますます高度化する中、マルウェアの中にはステルス性の高いものもあるため、一部の攻撃が成功しても不思議ではありません。マルウェアが配置されると、ネットワークからファイルを密かに盗み出すだけでなく、システムやネットワークに重大な損害を与える可能性があります。

内部関係者によるマルウェアインストール: 従業員または請負業者が（おそらく金銭的な利益のために）、組織のネットワークにマルウェアをインストールするように誘惑される場合があります。実際、AT&Tではマルウェアがインストールされ、その後5年間検出されませんでした。

セキュリティ上の懸念の解決

SecureAgeのSecureDataを使用した場合、マルウェアはデータを抽出することはできるかもしれませんが、盗まれたデータは暗号化されたままなので、悪意のある人物にとっては無意味なものになります。また、SecureAgeのSecureAPlusを併用すれば、許可されていないすべてのプロセス実行をブロックできることができます。つまり、上記シナリオの幹部は、有害なリンクを安全にクリックすることができたわけです。マルウェアはダウンロードされても、実行しようすれば、SecureAPlusがブロックしたでしょう。

1 Experian/Ponemonデータ侵害調査: 49% が新人研修中にトレーニングを実施。毎年トレーニングを実施していたのは、わずか24%

NIST カテゴリー 3
データセキュリティ

データ損失/リーク保護（DLP）

DLPは、ユーザーが重要な情報や機密情報を組織の外に送信しないことを目的としています。これは、これは、機密データがネットワークを通過するときに、それを認識してブロックしようとすることで実現されます。DLPの導入は、すべてのネットワーク資産とストレージの場所、および承認されたビジネスプロセスを包括的かつ正確に特定する必要がある、重要なプロジェクトです。

データ漏えいのシナリオ

不正な従業員がDLPシステムに対して、自分の行動は正当であると示します。DLPはビジネスコンテクストを認識していないので、このような行動は見過ごされて、データは流出してしまいます。

> General Electricから業界機密が盗まれ、その情報は夕焼けの画像のバイナリーコードに隠した状態で持ち出されました。このようなステガノグラフィーは、DLPシステムを掻い潜ります。

セキュリティ上の懸念

不完全なDLP構成: DLPの実装を成功させるためには、数多くの変数が関係します。システムの微調整に十分取り組まないと、不注意によるデータ漏洩が起きる一方で、データ損失の可能性のあるすべての手段を考慮しないと、機密情報盗難の頻繁な経路にもなります。DLPが機密データの流出を認識できない場合、その情報は漏洩して、制御不能になります。

セキュリティ上の懸念の解決

SecureAgeのSecureDataは、すべてのデータファイルを常に暗号化しているので、DLP構成の偶発的または故意による抜け穴があっても、データ損失は発生しません。SecureAgeを使用しても、パフォーマンスや操作性には影響を及ぼさないため、すべてを暗号化することは理にかなっています。ユーザーが、DLPに対して悪意のある活動を許可し、データの損失につながるような指示を出しても、暗号化されたデータが失われるだけで、組織の外では役に立ちません。

データの分類と権利の管理

データの分類システムは、情報へのアクセス範囲やセキュリティを定義するために使用されます。また、デジタル著作権を行使するために、適切に分類されたデータに暗号化を適用することができます。しかし、暗号化は実装が難しく、動作が遅く、使い方が難しいとされているため、一般的にはあまり使用されていません。

データ漏えいのシナリオ

ユーザーが機密文書を誤って分類した結果、データ保護レベルが低下してしまいます。ユーザーが情報を分類できるようにすると、プライバシーや情報セキュリティへの影響について、誤った判断をしてしまうことがあります。さらに、自動化された分類プロセスは確実なものではなく、企業は今日の「普通の」データが、明日の機密情報になる可能性があることを認識する必要があります。

> Desjardinsグループの不正な従業員は、自らの正当なユーザー認証情報を使用して、顧客アカウントデータおよそ290万件を盗み出しました。DLPは配備されていたと仮定されていますが、この機密情報のエクスポートを検出することはできませんでした

セキュリティ上の懸念

誤分類は、セキュリティの不適切さにつながる可能性: 前述の通り、機密性が高い文書や機密文書として分類された文書は、暗号化することで保護されることがあります。しかし、このセキュリティレベルが使いづらい場合、人々はこれを避けるようになります。また、人は簡単だからという理由で、文書を誤分類することもあります。自動分類プロセスは、設定された通りにしか機能しません。ファイルが「検出」されない場合、ファイルは分類されないため、適切に保護されません。さらに、データベースファイル、一時ファイル、およびログファイルは、機密情報が含まれていることが多いにもかかわらず、通常は分類されません。また、多くの分類·権限管理システムは、一般的に使用されるファイルタイプにのみ対応し、その他のファイルは完全に無視されます。なぜ、すべてが機密情報であると仮定しないのでしょうか?そうすれば、データセキュリティははるかにシンプルになるはずです。

セキュリティ上の懸念の解決

SecureAgeのSecureDataは、ファイルの種類に関係なくすべてが暗号化されるため、ITセキュリティの観点からは、データが正しく分類されているかどうかはもはや問題ではありません。SecureDataは、ユーザーに対して完全に透過的であるように設計されており、ユーザーはこれまで通りの方法で作業を行うことができます。パフォーマンスの低下やアプリケーションへの干渉もなく、ユーザーの手を煩わせることなく、データを強力に保護することができます。

データベースの暗号化

商用データベースの多くは、暗号化のオプションを提供しており、その多くは透過的データ暗号化（TDE）です。ただし、これは高価な上に、バージョン固有なため、ベンダー独自の管理システムで、データベースしか暗号化しません。

データ漏えいのシナリオ

機密情報を含むデータベースログまたは一時ファイルは、他の非構造化ファイルとともに保護されていないため、簡単にUSBなどのストレージにコピーが可能です。また、データベースがクラウドサービスに保存されている場合、安全な保護設定になっていない場合があります。クラウドデータベースが無防備であることを示すメディア報道は数多く存在します。

> ヨーロッパを代表するホテル予約プラットフォームのGekkoグループは、セキュリティで保護されていないデータベースから、顧客、クライアント、パートナーに関する1 TBを超えるデータを漏洩しました。それらのデータは、アカウントの乗っ取り、個人情報の盗難、金融詐欺にさらされることになりました。

セキュリティ上の懸念

非構造化ファイル、一時ファイル、ログファイルの盗難: ほとんどのデータベースアプリケーションは、非構造化ファイルをデータベースの外部に保存、管理されます。TDEはこれらのファイルを暗号化しません。また、一時ファイルやログファイルも作成されますが、これらのファイルには機密情報が含まれていることがよくあります。これらのファイルもTDEでは暗号化されません。

データベースファイルの盗難: 盗難者がデータベースを構成するファイルにアクセスできて、データベースが暗号化されていなければ、データは簡単に盗まれ、再構築されて、アクセスされます。

セキュリティ上の懸念の解決

SecureAgeのSecureDataでは、どのベンダーであっても、データベースにもアプリケーションにも影響を与えることなく、すべてのデータベースを暗号化することが可能です。データベースの操作中であっても、すべてのデータは暗号化されたままであるため、データベース ファイル盗難の脅威は軽減されます。

SecureDataは、ファイルの種類に関係なく、すべてのファイルを透過的に暗号化します。すべての非構造化ファイル、レポート、ログ、および一時ファイルは、データの盗難から自動的に保護されます。データベースからエクスポートされ、ローカルファイルに保存されたデータも暗号化されるため、盗まれたデータは組織の外では役に立ちません。

暗号化されたバックアップ

データバックアップ技術では、バックアップメディアを定期的に暗号化するか、少なくともパスワードで保護することが一般的です。これで、バックアップメディアの盗難からデータが保護されます。

データ漏えいのシナリオ

管理者が自分の「鍵」を使ってデータをバックアップ暗号化した場合、バックアップメディアは暗号化されますが、管理者は暗号化キーを保持しているため、常に保護されていないファイルをダウンロードが可能です。

セキュリティ上の懸念

管理者はバックアップを読み取り可能: 管理者は、必要なときにファイルを復元できるように、バックアップを復号する方法を知っている必要があります。つまり、特権を持つユーザーがバックアップにアクセスして、ファイルを盗み出すことは簡単です。

セキュリティ上の懸念の解決

SecureAgeのSecureDataであれは、すべてのファイルを根本から暗号化し、ファイルのライフサイクル全体にわたって暗号化を維持します。つまり、バックアップに暗号化されたファイルが含まれることになります。

管理者がバックアップからそのようなファイルを盗んでも、認証されたユーザーの鍵により暗号化されたままなので、役に立たないことがわかります。

> 米国のラジオ大手Entercomは、サードパーティーのクラウドホスティングサービスに保存していたデータベースのバックアップファイルに、権限のない管理者がアクセスできたことに気付き、これにRadio.comユーザーの認証情報が含まれていたと報告しました。
>
> キャセイパシフィック航空に対する50万ポンドの罰金は、バックアップファイルが保護されていない状態で保管されていることが判明したことに一因があります。

NIST カテゴリー 4
情報保護プロセスと手順

クラウドサービスのセキュリティ

クラウドサービスのセキュリティは、クラウドベースのシステム、データ、そしてインフラを守るために連携して機能する一連のポリシー、制御、手順、および技術で構成されています。クラウドサービスは、サードバーティにより運営されているため、自分のデータの安全はサードパーティに委ねていることになります。

データ漏えいのシナリオ

クラウドサービスに雇用されている管理人は、その特権的な地位を利用して、クラウド内のある会社のストレージバケット内のファイルにアクセスし、盗み見ることができます。

セキュリティ上の懸念

クラウドサービスの特権ユーザー: クラウドセキュリティは、外部からの不正アクセスと、サードパーティの特権ユーザーによる悪用を 防ぐ必要があります。しかし、特権ユーザーを直接管理することも、知ることも不可能です。

セキュリティ上の懸念の解決

組織のシステムを離れる前にデータを暗号化しましょう。SecureAgeのSecureDataを使用すれば、情報は完全に保護されます。クラウド管理者はファイルの存在を見ることはできても、データを覗き見したり、 アクセスしたりすることはできません。サービス、データベース、またはインフラの設定を誤ると、ファイルの盗難につながることはありますが、内部データは暗号化されたままなので使い物になりません。

> AWSに保存されていたCapital Oneの顧客情報1億件が何者かによって盗まれました。Amazonのエンジニアによるファイアウォール誤設定から、700以上のフォルダーのデータにリモートアクセスが発見されましたが、この継続的な盗難は 4ヶ月もの間、発覚しませんでした。

NIST カテゴリー 5
メンテナンス

ITセキュリティの基本的なアドバイスとして、システムの定期的なパッチ適用と保守が提唱されています。もちろん、これは優れたアドバイスです。

しかし、SecureAgeのSecureDataですべてのファイルを暗号化してしまえば、セキュリティパッチが完全に適用されていない（最新版でない）、脆弱性のあるサーバやデスクトップマシンでも、データ漏洩の心配は不要です。

NIST カテゴリー 6
保護テクノロジー

フルディスク暗号化

BitLockerおよび同様のシステムは、ディスクの中身を丸ごと暗号化します。

セキュリティ上の懸念

フルディスク暗号化を使用するシステムを稼働すると、ただちにすべてのユーザーとプロセスが、正当なものと悪意のあるものも含めて、復号したデータの形として、全てのファイルにアクセスすることが可能になります。つまり、フルディスク暗号化は、電車内で紛失したラップトップのデータを守るには優れていますが、稼働中のシステムには、何のセキュリティ上のメリットもありません。

セキュリティ上の懸念の解決

SecureAgeのSecureDataは、アクセス中も編集中も常にファイルの暗号化を保持します。システムの実行中は、権限を与えられた個人のみがデータを復号できます。また、他の場所にファイルがコピーされても、ファイルは暗号化は持続します。

SSLとTLS

SSLとTLSは、転送中のデータを暗号化して、安全を確保します。ほとんどのウェブサイトでは、トラフィックを傍受する人が有用なデータにアクセスできないように、この種のセキュリティが使用されています。

セキュリティ上の懸念

サーバーからクライアントへの受け渡し時、情報は暗号化されています。しかし、サーバーに保存されているデータ、およびクライアントシステムに保存されている情報は、SSL/TLSでは保護されません。

セキュリティ上の懸念の解決

SecureAgeのSecureDataを使用すれば、ファイルは常に暗号化されます。つまり、転送中だけでなく、使用中および保管中にも保護されるようになります。

> Nedbankはサードパーティーでのサービスプロバイダにおいて、170万件の顧客記録を流出するセキュリティ侵害を受けました。データはSSL/TLSで送信されたものの、暗号化されずに保存されていました。

マルウェア対策システム

マルウェアやランサムウェアの攻撃が「成功した」という報道が多いのはなぜでしょうか？マルウェア対策だけではすべてを防ぐことはできないと考え、企業は時間と費用をかけ、サイバーセキュリティについて、また悪意のあるものをクリックしたり開いたりすることの危険性について、従業員に教育してるのにもかかわらず。

データ漏えいのシナリオ

ハッカー（または内部関係者）がネットワーク上にマルウェアを展開し、バックドアを開くことに成功しました。

マルウェアは、企業の防御を回避したり、被害者の特権を利用したりすることが分かっています。いずれにせよ、データへのアクセスが可能となり、ファイルの流出が容易になります。

> Norske Hydroはランサムウェア攻撃を受け、システムロックアウト後の復旧に、約6000万ポンドのコストがかかりました。SecureAPlusがインストールされていれば、マルウェアの実行は許可されず、犯人はITサービスに損害を与えることができなかったでしょう。

セキュリティ上の懸念

マルウェアは一歩先を行っています: ランサムウェアはAPT(Advanced Persistent Threat)へと進化し、現在、組織に損害を与え、将来にわたって金銭を強要し続けようとする「ディスラプションウェア」が登場しています。

ゼロデイ攻撃と機械学習技術を使用して、ハッカーは、マルウェア対策製品よりも数歩先を進んでいます。マルウェアを認識したり、進行中の悪意のある動作を特定したりする従来のアプローチでは、常に何かを見過ごしてしまう可能性があります。

セキュリティ上の懸念の解決

SecureAgeのSecureDataは、すべてのデータファイルを常に暗号化して保持するため、データを盗もうとするマルウェアは、暗号化された情報を盗み出すことになります。しかし、組織の外に流出した暗号化データは、窃盗犯にとっては無用の長物でしかありません。この機会に、SecureAgeのSecureAPlusを再度ご紹介しましょ う。SecureAPlusは、ホワイトリストとアプリケーション コントロールを使用して、許可されていないプロセスをすべてブロックします。つまり、マルウェアの実行を許可しないので、問題を起こすマルウェアを完全に回避することができます。

結論

これまで、サイバーセキュリティのフレームワークの中で一般的に使用されているITセキュリティ技術について説明してきましたが、何重もの技術でデータを保護していても、データ盗難の被害は絶えず発生していることがわかりました。犯人（外部または内部）が、これらの防御を回避してしまえば、盗まれたファイル内の情報は完全に保護が解かれた状態です。

SecureAgeは、データファイルがどこに保存されていてもすべてを暗号化します。データ自体を本質的に目に見えない形で暗号化することにより、既存のサイバーセキュリティ層を強化し、盗まれてしまったデータも無用の長物と化してしまいます。盗まれたデータを組織の外では使えないようにする（復号できない）ことで、規制や法律の遵守、ブランド毀損、事業回復といった、データ侵害による被害を軽減することができます。

SecureAgeのアプローチは、機密性・秘密性の高い情報を確実に保護することを可能にします。

SecureAge Technology

SecureAge Technologyは、シンガポールに本社を置き、真のセキュリティと使いやすさを両立させるデータセキュリティ企業です。SecureDataは、PKIセキュリティ技術を改良したものがベースで、シンガポール政府向けに2003年に最初のバージョンがリリースされました。SecureAgeは、特許取得済みのPKI ベースの暗号化を、まるで元々備わっているかのような透過的なデータ保護コンポーネントとしてまとめ上げたもので、瞬く間にデータ暗号化パートナーとしてその他の政府機関や公共機関からも選ばれるようになりました。こうした顧客との長期的かつ深く密接な関係を通して、SecureAgeは大規模かつ複雑な組織のデータ保護に関する幅広い経験を得ることができました。

SecureAgeのデータセキュリティソリューションは、公共機関や民間企業がそのネットワーク内のデータ移動を完全に制御できるようにします。すべてのファイルを、いつでも、どこでも。

SecureAgeのセキュリティ製品は、最高レベルのデータ保護が求められる組織にお選びいただいています。顧客には、シンガポール、香港、および日本の政府系機関や、ブリティッシュ·アメリカン·タバコ、ソニー、成田エアポートテクノ、タイ政府貯蓄銀行、GRG Bankingなどが含まれます。

SecureAge Technology: データセキュリティへのアプローチ

予防的なデータ保護

データセキュリティ

データセキュリティとは、広範な暗号化を意味します。データの保護は、最も基本的であり、自己完結型の単位であるファイル上で実施する必要があります。他社から提供されているソリューションでは、一部のデータのみを一定期間のみ保護したり、セキュリティよりもコンプライアンスに重点が置かれていたり、また導入することで複雑性が増し、逆にリスクが生じたりしています。また元から内部にいるユーザー（どのシステムでも最も脆弱な部分）に対しては、境界防御を施すだけでは不十分です。

アプリケーションの整合性

アプリケーションの整合性とは、ホワイトリスト（許可リスト）と、アプリケーションへのデータの結び付けによる制御を意味します。認証されたプロセスのみが、特定の目的で特定のデータにアクセスできる状態にすべきです。従来のマルウェア対策システムは受け身的な保護の代表的なもので、それでは手遅れです。システムの焦点は既知のマルウェアに置かれ、既にアクティブな状態である、悪意のあるプロセスを阻止しようとするためです。

ユーザビリティ

ユーザビリティとは、本質的で意識されない透過的テクノロジーを意味します。ソリューションにおいては、人的要素を構成要素として含めたり、変えようとするのではなく、完全に排除する必要があります。トレーニングやモニタリングは常に機能するわけではなく、ソリューションが自然でないと、人は独自の（セキュアではない）方法を編み出すものです。ユーザーは、他の点について考慮することなく、思い通りにまたは必要に応じて作業できる必要があります。

トレードオフなし

SecureAgeでは、これらの原則の間にトレードオフはありません。特に、データセキュリティを強化するためにユーザビリティが犠牲になることはありません。適切な方法が難しい場合、人は何かを達成するために他の方法を見つけるものであることを認識し、それを基本原則としてSecureAgeの製品設計を行っています。

詳細を見る

その他のホワイトペーパーは、こちらからご覧いただけます。SecureAgeのエンタープライズ向けデータセキュリティソリューションの詳細は、当社までお問い合わせください。データのセキュリティを向上させ、無料トライアルを手配する方法について、喜んでご相談させていただきます。お問い合わせください。

ウェブサイト www.secureage.com

SecureAge

シンガポール 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
英国 74 Mackie Avenue, Brigton, BNI 8RB, Company No. 11734665
日本 105-0001 東京都港区虎ノ門1-16-6 UCF7F
北米 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA